Specifically, under this legislation, contractors would have to provide a bill of materials that identifies each part or component of the software supplied to DHS and take steps to ensure that each item is free from known security vulnerabilities or defects.

The bill of materials process is akin to the listing of ingredients on a package of food.

Once DHS has this detailed supply chain information, it will have far greater visibility into what it is purchasing and installing on its networks.

□ 1545

With this information, DHS can take more timely action to mitigate risks associated with software on its network.

Importantly, H.R. 4611, which was introduced by my colleague from New York (Mr. TORRES), requires DHS to instruct personnel on how to enforce the new requirements to hold contractors accountable.

Finally, the bill requires the Government Accountability Office to review the department-wide guidance and assess how it aligns with President Biden's recent executive order on improving the Nation's cybersecurity.

As the President stated in this order, the Federal Government must take decisive steps to modernize its approach to cybersecurity to keep pace with today's dynamic and increasingly sophisticated cyber threat environment.

I could not agree more.

Enactment of H.R. 4611 would be a decisive step toward improving DHS's ability to prevent, detect, and respond to cyberattacks on its own networks.

I urge my colleagues to support this legislation and reserve the balance of my time.

Mr. GUEST. Madam Speaker, I yield myself such time as I may consume.

Madam Speaker, I rise today in support of H.R. 4611, the DHS Software Supply Chain Risk Management Act of 2021.

As we have seen over the past year, our software supply chains are increasingly vulnerable. It is vital that the Department of Homeland Security does its part to ensure that software in use by the Department and its contractors is secure.

This legislation will help DHS better understand and track the software and systems in use by its contractors so that it can better mitigate risk within the software supply chain.

I urge Members to join me in supporting H.R. 4611, and I reserve the balance of my time.

Mr. THOMPSON of Mississippi. Madam Speaker, I yield 2 minutes to the gentleman from New York (Mr. TORRES), the vice chair of the Committee on Homeland Security and the sponsor of the bill.

Mr. TORRES of New York. Madam Speaker, a cyberattack on a software supply chain is like an infectious disease outbreak, spreading widely and rapidly, and causing untold damage far and wide.

The SolarWinds espionage campaign against the United States, which spread surreptitiously through a software product, represents the greatest intrusion into the Federal Government in the history of the United States.

SolarWinds should serve as a wake-up call. The United States Government can no longer take for granted the safety of the software it uses. The Federal Government must be proactive in identifying and correcting cyber vulnerabilities; and as the lead agency on cybersecurity, DHS in particular must emerge as the gold standard.

I am therefore proud to partner, on a bipartisan basis, with my colleague, the gentleman from New York (Mr. GARBARINO), to pass H.R. 4611, the DHS Software Supply Chain Risk Management Act of 2021.

H.R. 4611 would require the DHS Under Secretary for Management to issue department-wide guidance that in turn requires DHS contractors to submit a software bill of materials, identifying the origin of each component of software provided to DHS.

DHS should know the precise origin of the software it uses; whether a software component comes from a questionable firm that fails to follow best practices in cybersecurity; whether it comes from a hostile nation-state intent on planting back doors.

Homeland security can easily die in darkness, and the purpose of H.R. 4611 is to bring greater light, greater transparency to the software supply chains which for far too long have been left wide open to cyber espionage and sabotage. We owe it to ourselves to learn from the experience of SolarWinds, for those who fail to learn from history are doomed to repeat it.

Mr. GUEST. Madam Speaker, I have no further speakers, and I urge Members to support this bill. I yield back the balance of my time.

Mr. THOMPSON of Mississippi. Madam Speaker, I yield myself the balance of my time to close.

As the lead Federal agency for cybersecurity, DHS has taken steps to increase public awareness of software vulnerabilities routinely exploited by malicious cyber actors.

To identify and manage these types of vulnerabilities on its own network, DHS needs better visibility into the supply chains of the software it procures.

Enactment of H.R. 4611 would ensure that DHS has access to the information it needs to enhance its ability to manage the risks to its own networks.

I urge my colleagues to support H.R. 4611, and I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Mississippi (Mr. THOMPSON) that the House suspend the rules and pass the bill, H.R. 4611, as amended.

The question was taken.

The SPEAKER pro tempore. In the opinion of the Chair, two-thirds being in the affirmative, the ayes have it.

Mr. POSEY. Madam Speaker, on that I demand the yeas and nays.

The SPEAKER pro tempore. Pursuant to section 3(s) of House Resolution 8, the yeas and nays are ordered.

Pursuant to clause 8 of rule XX, further proceedings on this motion are postponed.

DARREN DRAKE ACT

Mr. THOMPSON of Mississippi. Madam Speaker, I move to suspend the rules and pass the bill (H.R. 4089) to direct the Secretary of Homeland Security to develop and disseminate best practices for rental companies and dealers to report suspicious behavior to law enforcement agencies at the point of sale of a covered rental vehicle to prevent and mitigate acts of terrorism using motor vehicles, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 4089

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Darren Drake Act''.

SEC. 2. BEST PRACTICES RELATED TO CERTAIN INFORMATION COLLECTED BY RENTAL COMPANIES AND DEALERS.

(a) DEVELOPMENT AND DISSEMINATION.—

(1) IN GENERAL.—Not later than one year after the date of the enactment of this Act, the Secretary of Homeland Security shall develop and disseminate best practices for rental companies and dealers to report suspicious behavior to law enforcement agencies at the point of sale of a covered rental vehicle.

(2) CONSULTATION; UPDATES.—The Secretary shall develop and, as necessary, update the best practices described in paragraph (1) after consultation with Federal, State, local, and Tribal law enforcement agencies and relevant transportation security stakeholders.

(3) GUIDANCE ON SUSPICIOUS BEHAVIOR.—The Secretary shall include, in the best practices developed under paragraph (1), guidance on defining and identifying suspicious behavior in a manner that protects civil rights and civil liberties.

(b) REPORT TO CONGRESS.—Not later than one year after the date of the enactment of this Act, the Secretary of Homeland Security shall submit to Congress a report on the implementation of this section, including an assessment of—

(1) the impact of the best practices described in subsection (a) on efforts to protect the United States against terrorist attacks; and

(2) ways to improve and expand cooperation and engagement between—

(A) the Department of Homeland Security;

(B) Federal, State, local, and Tribal law enforcement agencies; and

(C) rental companies, dealers, and other relevant rental industry stakeholders.

(c) DEFINITIONS.—In this section:

(1) The terms ''dealer'' and ''rental company'' have the meanings given those terms in section 30102 of title 49, United States Code.

(2) The term ''covered rental vehicle'' means a motor vehicle that—

(A) is rented without a driver for an initial term of less than 4 months; and

(B) is part of a motor vehicle fleet of 35 or more motor vehicles that are used for rental purposes by a rental company.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from

Mississippi (Mr. THOMPSON) and the gentleman from Mississippi (Mr. GUEST) each will control 20 minutes.

The Chair recognizes the gentleman from Mississippi (Mr. THOMPSON).

GENERAL LEAVE

Mr. THOMPSON of Mississippi. Madam Speaker, I ask unanimous consent that all Members may have 5 legislative days in which to revise and extend their remarks and include extraneous material on this measure.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from Mississippi?

There was no objection.

Mr. THOMPSON of Mississippi. Madam Speaker, I yield myself such time as I may consume.

Madam Speaker, I rise today in support of H.R. 4089, the Darren Drake Act.

This month the Nation observed the 20th anniversary of the September 11th attacks. Next month we mark the fourth anniversary of the deadliest terrorist attack to be carried out in New York City since the 9/11 attacks.

In that attack, a lone wolf, inspired by ISIS, rammed a rented truck into pedestrians and cyclists who were out enjoying a sunny Halloween afternoon on a pathway that ran along the Hudson River.

That attack took the lives of 8 people and injured 11 others. One of the victims of the attack was Darren Drake, a 32-year-old bicyclist and the namesake for this important legislation.

While it is not within our power to bring back Darren Drake or the seven other victims of this tragedy, we do have the ability to learn from this event to better address the threats of vehicle-based attacks.

H.R. 4089, introduced by my colleague from New Jersey (Mr. GOTTHEIMER), seeks to ensure that rental vehicle facilities, like the one where Darren Drake's killer rented a truck, are better equipped to prevent vehicle-based attacks.

Specifically, the Darren Drake Act requires the Department of Homeland Security to develop best practices for vehicle rental companies and dealers to report suspicious behavior in a manner that protects civil rights and civil liberties.

The bill directs DHS to consult and share best practices with State and local partners and rental companies to help strengthen communication and relationships to guard against vehicle-based attacks.

H.R. 4089 is a commonsense measure that acknowledges that vehicle rental companies are important partners in efforts to prevent vehicle-based terrorist attacks and provide them with the tools to identify suspicious behavior and notify authorities.

I urge my colleagues to support the Darren Drake Act and reserve the balance of my time.

Mr. GUEST. Madam Speaker, I yield myself such time as I may consume.

Madam Speaker, I rise today in support of H.R. 4089, the Darren Drake Act.

In the wake of the Taliban takeover of Afghanistan, it is critical that we remain vigilant to threats posed by terrorists and extremist organizations.

Over the past two decades, terrorists have carried out multiple vehicle-ramming attacks in North America and Western Europe.

Al-Qaida and ISIS have promoted these type of attacks for years, including in Inspire, the online magazine of al-Qaida, and Rumiya, ISIS's magazine.

ISIS has called upon its followers to conduct vehicle-ramming attacks by buying, renting, stealing, or borrowing trucks and targeting large outdoor events, crowded pedestrian streets, outdoor markets, and rallies.

This legislation requires the Department of Homeland Security to develop and disseminate best practices for rental companies and dealers to report suspicious behavior to law enforcement agencies at the point of sale of a covered rental vehicle to prevent and mitigate acts of terrorism using these motor vehicles.

This represents an important tool for addressing extremist threats—the ability of government and the private sector to work together to mitigate terrorism risk.

I urge Members to join me in supporting H.R. 4089, and I reserve the balance of my time.

Mr. THOMPSON of Mississippi. Madam Speaker, I yield 3 minutes to the gentleman from New Jersey (Mr. GOTTHEIMER), the sponsor of this bill.

Mr. GOTTHEIMER. Madam Speaker, I rise today in support of H.R. 4089, the Darren Drake Act, bipartisan legislation I introduced in the Committee on Homeland Security with my Republican colleague and co-chair of the Problem Solvers Caucus, the gentleman from Pennsylvania (Mr. FITZPATRICK), to help prevent terrorist vehicle attacks and to protect Americans nationwide.

This legislation is named in memory of a constituent from my district, Darren Drake from New Milford, New Jersey, who was one of those tragically killed in the terrorist attack in Lower Manhattan on October 31, 2017, when an ISIS-inspired terrorist drove a rented pickup truck into cyclists and runners for one mile along the West Side Highway, killing eight.

The bill takes critical steps to stop these weapons of terror and help prevent terrorist truck attacks by requiring the Department of Homeland Security to develop and disseminate best practices for vehicle rental companies and dealers to report suspicious behavior to law enforcement.

These best practices will be developed and updated in consultation with State and local law enforcement as well as industry experts.

This crucial legislation will provide rental companies and car dealers with the vital information they need to flag and stop potential terrorist threats in their tracks. We can take no chances when it comes to terrorism, which is why this bill will help ensure all rental companies report suspicious behavior at every point of sale. No excuses. We simply cannot afford any excuses when it comes to a question of life or death.

The bill will also require the Secretary of Homeland Security to report to Congress regarding the implementation of these best practices and other ways they are helping improve coordination between the Department and rental vehicle providers.

This commonsense, bipartisan bill is aimed at stopping ISIS-inspired, lone wolf, and domestic terrorists from easily trucks and other vehicles to wreak havoc and cause mass destruction and health. It is an important addition to our arsenal as we work to eradicate threats of terror across our Nation.

I want to thank Darren's parents, Jimmy and Barbara Drake, who have become dear friends, for working with me on this effort. I thank them for their leadership. We will continue working to ensure this measure becomes law, in Darren's memory and honor, to help prevent future attacks and save lives. It is the least we can do.

Madam Speaker, I strongly urge all my colleagues to support this commonsense, bipartisan legislation to help our Nation fully combat terror wherever it rears its ugly head.

Mr. GUEST. Madam Speaker, I have no further speakers, and I urge Members to support this bill. I yield back the balance of my time.

Mr. THOMPSON of Mississippi. Madam Speaker, I yield myself the balance of my time to close.

Madam Speaker, from the 2016 Bastille Day truck attack in France to the 2017 deadly car ramming in Charlottesville to the 2017 attack that took the lives of Darren Drake and seven others, we have seen the use of vehicles to carry out terrorist attacks become disturbingly common.

Our Nation faces a complex and evolving threat landscape. But the threat of vehicle-ramming attacks is not going away.

As long as would-be terrorists seek to use rental vehicles as weapons of terror, we must provide rental dealers with the ability to do their part.

I urge my colleagues to support the Darren Drake Act, and I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Mississippi (Mr. THOMPSON) that the House suspend the rules and pass the bill, H.R. 4089, as amended.

The question was taken.

The SPEAKER pro tempore. In the opinion of the Chair, two-thirds being in the affirmative, the ayes have it.

Mr. POSEY. Madam Speaker, on that I demand the yeas and nays.

The SPEAKER pro tempore. Pursuant to section 3(s) of House Resolution 8, the yeas and nays are ordered.

Pursuant to clause 8 of rule XX, further proceedings on this motion are postponed.

□ 1600

K–12 CYBERSECURITY ACT OF 2021

Mr. THOMPSON of Mississippi. Madam Speaker, I move to suspend the rules and pass the bill (S. 1917) to establish a K–12 education cybersecurity initiative, and for other purposes.

The Clerk read the title of the bill.

The text of the bill is as follows:

S. 1917

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''K–12 Cybersecurity Act of 2021''.

SEC. 2. FINDINGS.

Congress finds the following:

(1) K–12 educational institutions across the United States are facing cyber attacks.

(2) Cyber attacks place the information systems of K–12 educational institutions at risk of possible disclosure of sensitive student and employee information, including—

(A) grades and information on scholastic development;

(B) medical records;

(C) family records; and

(D) personally identifiable information.

(3) Providing K–12 educational institutions with resources to aid cybersecurity efforts will help K–12 educational institutions prevent, detect, and respond to cyber events.

SEC. 3. K–12 EDUCATION CYBERSECURITY INITIATIVE.

(a) DEFINITIONS.—In this section:

(1) CYBERSECURITY RISK.—The term ''cybersecurity risk'' has the meaning given the term in section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659).

(2) DIRECTOR.—The term ''Director'' means the Director of Cybersecurity and Infrastructure Security.

(3) INFORMATION SYSTEM.—The term ''information system'' has the meaning given the term in section 3502 of title 44, United States Code.

(4) K–12 EDUCATIONAL INSTITUTION.—The term ''K–12 educational institution'' means an elementary school or a secondary school, as those terms are defined in section 8101 of the Elementary and Secondary Education Act of 1965 (20 U.S.C. 7801).

(b) STUDY.—

(1) IN GENERAL.—Not later than 120 days after the date of enactment of this Act, the Director, in accordance with subsection (g)(1), shall conduct a study on the specific cybersecurity risks facing K–12 educational institutions that—

(A) analyzes how identified cybersecurity risks specifically impact K–12 educational institutions;

(B) includes an evaluation of the challenges K–12 educational institutions face in—

(i) securing—

(I) information systems owned, leased, or relied upon by K–12 educational institutions; and

(II) sensitive student and employee records; and

(ii) implementing cybersecurity protocols;

(C) identifies cybersecurity challenges relating to remote learning; and

(D) evaluates the most accessible ways to communicate cybersecurity recommendations and tools.

(2) CONGRESSIONAL BRIEFING.—Not later than 120 days after the date of enactment of this Act, the Director shall provide a Congressional briefing on the study conducted under paragraph (1).

(c) CYBERSECURITY RECOMMENDATIONS.—Not later than 60 days after the completion of the study required under subsection (b)(1), the Director, in accordance with subsection (g)(1), shall develop recommendations that include cybersecurity guidelines designed to assist K–12 educational institutions in facing the cybersecurity risks described in subsection (b)(1), using the findings of the study.

(d) ONLINE TRAINING TOOLKIT.—Not later than 120 days after the completion of the development of the recommendations required under subsection (c), the Director shall develop an online training toolkit designed for officials at K–12 educational institutions to—

(1) educate the officials about the cybersecurity recommendations developed under subsection (c); and

(2) provide strategies for the officials to implement the recommendations developed under subsection (c).

(e) PUBLIC AVAILABILITY.—The Director shall make available on the website of the Department of Homeland Security with other information relating to school safety the following:

(1) The findings of the study conducted under subsection (b)(1).

(2) The cybersecurity recommendations developed under subsection (c).

(3) The online training toolkit developed under subsection (d).

(f) VOLUNTARY USE.—The use of the cybersecurity recommendations developed under (c) by K–12 educational institutions shall be voluntary.

(g) CONSULTATION.—

(1) IN GENERAL.—In the course of the conduction of the study required under subsection (b)(1) and the development of the recommendations required under subsection (c), the Director shall consult with individuals and entities focused on cybersecurity and education, as appropriate, including—

(A) teachers;

(B) school administrators;

(C) Federal agencies;

(D) non-Federal cybersecurity entities with experience in education issues; and

(E) private sector organizations.

(2) INAPPLICABILITY OF FACA.—The Federal Advisory Committee Act (5 U.S.C App.) shall not apply to any consultation under paragraph (1).

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from Mississippi (Mr. THOMPSON) and the gentleman from Mississippi (Mr. GUEST) each will control 20 minutes.

The Chair recognizes the gentleman from Mississippi (Mr. THOMPSON).

GENERAL LEAVE

Mr. THOMPSON of Mississippi. Madam Speaker, I ask unanimous consent that all Members have 5 legislative days to revise and extend their remarks and to include extraneous material on this measure.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from Mississippi?

There was no objection.

Mr. THOMPSON of Mississippi. Madam Speaker, I yield myself such time as I may consume.

Madam Speaker, in the past few weeks, millions of students have returned to school across the country. The range of public health, safety, and security risks that schools face today is truly astounding.

In recent years, schools have increasingly been subjected to ransomware attacks where cybercriminals lock networks and demand ransom payments, sometimes while threatening to release sensitive information, including students' personal data.

According to the K–12 Cybersecurity Resource Center, in 2020 alone, there were over 480 publicly disclosed cyber incidents at schools in the United States, an 18 percent increase over the previous year.

Notably, the rate of such incidents increased in the second half of last year as COVID–19 forced schools to shift to virtual learning, creating new risks, such as the disruption of online classes and online school meetings.

The impacts of ransomware attacks on schools have included the cancellation of classes, the release of sensitive information, like the name of a 9-year-old student being evaluated for a disability, and costs as high as $7.7 million for Baltimore County schools to respond to and recover from a November 2020 attack.

With many schools still operating under virtual or hybrid conditions because of the ongoing COVID–19 pandemic, the vulnerabilities to such cyberattacks are even greater.

In December, the FBI Cybersecurity and Infrastructure Security Agency, or CISA, and the Multi-State Information Sharing and Analysis Center released a joint cybersecurity advisory to alert schools to the increase in cyber threats and provide best practices on how to reduce the risk of such incidents.

To further assist K–12 schools, we must do more to help schools guard against cyber threats.

S. 1917, the K–12 Cybersecurity Act, introduced by Senator GARY PETERS from Michigan, requires CISA to conduct a study of the cybersecurity risks facing K–12 educational institutions and develop recommendations based on that study.

By developing an online training tool kit for schools, and making the study and recommendations publicly available, CISA will be able to provide schools with targeted information to better protect their networks and reduce their cybersecurity risk.

An identical version of this legislation was introduced in the House by the gentleman from Rhode Island (Mr. LANGEVIN) and cosponsored by Representatives MATSUI, SLOTKIN, GARBARINO, and CLYDE. The House measure was reported favorably by the Homeland Security Committee by voice vote in July.

Passing S. 1917 today would send this bill to the President for signature, allowing CISA to begin this important work to better secure our schools.

Mr. Speaker, I urge my colleagues to support this legislation, and I reserve the balance of my time.

Mr. GUEST. Mr. Speaker, I yield myself such time as I may consume.

I rise today in support of S. 1917, the K–12 Cybersecurity Act of 2021.

Schools around our country are increasingly the target of malicious cyber actors and have recently been targeted with a deluge of ransomware attacks.